United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

The United States Marine Corps in Cyberspace:
Every Marine a Cyber Warrior

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

Major Eugene M. Wall, USAF

AY 07-08

Mentor and Oral Defense Committee Member: Richard L. DiNardo, PhD.
Approved: _____
Date: 16 April 2008

Oral Defense Committee Member: Paul D. Gelpi, PhD.
Approved: _____
Date: 16 April 2008

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2008		**00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The United States Marine Corps in Cyberspace: Every Marine a Cyber Warrior	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps, Command Staff College,Marine Corps University, 2076 South Street,Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**42**	

Executive Summary

Title: The Importance of the United States Marine Corps in Defending Cyberspace: Every Marine a Cyber Warrior

Author: Major Eugene M. Wall, United States Air Force

Thesis: The threats in cyberspace will hinder the Marine Corps from accomplishing its future missions unless every Marine takes an active roll in defending the operating environment of cyberspace.

Discussion: Dr. Lani Kass best summed up the current state of military operational requirements when she said, "If we don't dominate cyberspace, we won't be able to dominate air, space, land or sea domains." This statement drives home the point for the Marine Corps that in order to be the an expeditionary force in readiness, capable of exploiting the efficiency and lethality of the Marine Air Ground Task Force (MAGTF), the Marine Corps must play an active roll in the DoD effort to dominate cyberspace. Future concepts for the Marine Corps rely on a secure cyber operating environment in order to employ the MAGTF. The responsibility for defense of cyberspace, is not solely the responsibility of organizations such as the Marine Corps Network Operations and Security Center, nor any other computer network control center. The responsibility actually falls on every Marine to participate in order to ensure the MAGTFs freedom of maneuver in cyberspace, and deny adversaries around the globe their freedom to maneuver. This study highlights the threats from cyberspace that will induce friction in future operating environments. It is meant to provide Marines with just enough knowledge to inspire them to consider the threat when planning and executing future operations.

Conclusion: The threats from cyberspace are significant enough to hinder the Marine Corps' ability to accomplish its mission. It is the synergistic effects of every Marine's actions in defending cyberspace that will allow for military dominance in cyberspace, and thus the dominance of air, space, land, and sea.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Illustrations

Table of Contents

Preface

Cyberspace has come to the forefront in the past decade as a medium that supports the global economy, facilitates socialization, and provides a means to broadcast information at speeds never before seen. It has also become a favorite battle ground for criminals and terrorists. The Marine Corps is a target of malicious actions in cyberspace. Over the past year I have observed a full spectrum of opinions relating to the significance of malicious activity in cyberspace and its relationship to the ability of the Marine Corps to accomplish it's future missions. Opinions given to me about this topic ranged from views that cyber defense is the key to mission success, to the opposite end that claim that cyberspace has nothing to do with finding, closing, and destroying an enemy, or pacifying the local population. I personally believe the answer lies somewhere in the middle, but feel it is necessary that everyone has a role, and that everyone at least understand their part in this effort. With no other compelling papers written for the Marine Corps on this topic, I felt compelled to write this and try to inspire those individuals who do not believe they have a roll in the defense of cyberspace to understand the complexity and necessity of this mission.

Through the course of this journey I received a lot of help from people at Quantico Marine Corps Base. I would like to express my sincere appreciation to Colonel Eric Rolaf, Commander of the Marine Corps Network Operations and Security Center, and his staff, specifically Lieutenant Colonel Augusto Catta, Mr. Paul Skopowski, and Mr. Dave Dean. Furthermore, I would also like to thank Lieutenant Colonel Steve Roberts and Capt Stephanie Arndt of the Marine Corps Combat Development Command for assisting in understanding the role of cyberspace in future Command and Control concepts.

REPORT DOCUMENTATION PAGE

FORM APPROVED - - - OMB NO. 0704-0188

1. AGENCY USE ONLY *(LEAVE BLANK)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED *STUDENT RESEARCH PAPER*

4. TITLE AND SUBTITLE The United States Marine Corps in Cyberspace: Every Marine a Cyber Warrior	5. FUNDING NUMBERS *N/A*
6. AUTHOR(S) Maj Eugene M. Wall	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) *USMC COMMAND AND STAFF COLLEGE* *2076 SOUTH STREET, MCCDC, QUANTICO, VA 22134-5068*	8. PERFORMING ORGANIZATION REPORT NUMBER *NONE*
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) *SAME AS #7.*	10. SPONSORING/MONITORING AGENCY REPORT NUMBER: *NONE*
11. SUPPLEMENTARY NOTES *NONE*	
12A. DISTRIBUTION/AVAILABILITY STATEMENT *NO RESTRICTIONS*	12B. DISTRIBUTION CODE *N/A*

ABSTRACT *(MAXIMUM 200 WORDS)*
Dr. Lani Kass best summed up the current state of military operational requirements when she said, "If we don't dominate cyberspace, we won't be able to dominate air, space, land or sea domains." This statement drives home the point for the Marine Corps that in order to be the an expeditionary force in readiness, capable of exploiting the efficiency and lethality of the Marine Air Ground Task Force (MAGTF), the Marine Corps must play an active roll in the DoD effort to dominate cyberspace. Future concepts for the Marine Corps rely on a secure cyber operating environment in order to employ the MAGTF. The responsibility for defense of cyberspace, is not solely the responsibility of organizations such as the Marine Corps Network Operations and Security Center, nor any other computer network control center. The responsibility actually falls on every Marine to participate in order to ensure the MAGTFs freedom of maneuver in cyberspace, and deny adversaries around the globe their freedom to maneuver. This study highlights the threats from cyberspace that will induce friction in future operating environments. It is meant to provide Marines with enough knowledge to inspire them to consider the threat when planning and executing future operations.

14. SUBJECT TERMS (KEY WORDS ON WHICH TO PERFORM SEARCH) Cyberspace	15. NUMBER OF PAGES:
	16. PRICE CODE: N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE:	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	*UNCLASSIFIED*	*UNCLASSIFIED*	

I. INTRODUCTION

"We are in a world today where, in addition to the classical dimension of land, sea, and air, we have a virtual dimension called cyberspace."[1] These words echoed across a Washington D.C. audience at the Center for Strategic and International Studies. The speaker was not representing a major information technology firm trying to explain a notional threat in order to sell a product. Rather, the speaker was Jaak Aaviksoo, a theoretical physicist and the defense minister of Estonia. His presentation and proclamation were based on practical experience. For three weeks in April and May 2007 a cyber attack from outside of Estonia brought the nation to a standstill. Government operations were ineffective in their efforts to direct a rapid recovery from the attack. The two banks that held nearly 90 percent of the nations economy were breached. The Estonian population felt the psychological impact of a war that produced no traditional casualties.[2]

Globalization in a post-Cold War era, aided by advances in information technology, have expanded the requirements for national security beyond traditional diplomatic, economic, and military roles. Security concerns now extend beyond the physical world to the nebulous world of cyberspace.[3]

In the 21st Century a new medium for the global economy and security has emerged and the United States military finds itself at the forefront of protecting the new domain. This new domain and battlefield is cyberspace. Cyberspace, however, is not solely used as a medium to translate the global economy; it is used as a medium to enable the warfighting functions of the world's militaries.

The United States Department of Defense (DoD) has already commenced military operations in cyberspace. The United States Strategic Command (STRATCOM), with support from the military services and other national level agencies, is organizing an effort to protect the United States from cyber threats. The mission associated with cyber defense is nothing like the United States Marine Corps has encountered in its history. Furthermore, conducting operations to defend cyberspace is not an explicit task associated with the mission of being an expeditionary force in readiness. With such a vast commitment on the part of the DoD and joint community to defend cyberspace, it is imperative that we answer the question of whether or not there is a credible threat in cyberspace preventing the Marine Corps from being an expeditionary force in readiness for the future. Additionally, if there are threats in cyberspace challenging the ability of the Marine Corps from succeeding in its mission, what are the impacts of those threats why is it important to engage the threat? This paper will set out to explore these questions in order to illustrate the point that the threats in cyberspace will hinder the Marine Corps from accomplishing its future missions unless every Marine takes an active role in defending the operating environment of cyberspace.

II. WORDS MEAN THINGS

Before cyberspace became a military term it was introduced to the world in 1984 by William Gibson in his book *Neuromancer*.[4] By the mid 1990's the DoD introduced the term into its vernacular as numerous papers were written at Air University and the Naval War College on the potential for future military operations in cyberspace. In these papers it is virtually impossible to find a unified definition of what cyberspace meant to the authors. Today, the definition of cyberspace still varies depending on the reference.

The DoD defines cyberspace as, "the notional environment in which digitized information is communicated over computer networks."[5] The United States Air Force definition varies slightly. According to Air Force Doctrine Document 1-2 cyberspace is, "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data via networked information systems and associated physical infrastructures."[6] The United States Marine Corps and Army do not have a formal definition for cyberspace.[7]

The subtle differences between the definitions are significant. The first is noted in the characterization of cyberspace. The DoD definition implies a medium that is not real compared to the physical medium of the traditional land, sea, air, and space battle domains. The Air Force characterizes cyberspace simply as a domain. The American Heritage Dictionary defines a domain as a territory over which rule or control is exercised.[8]

Maneuver in cyberspace cannot be manipulated or controlled just as militaries control maneuver over geographic land. At this time it is easier to define the boundaries of space than the boundaries of cyberspace as we have physical laws that govern maneuver in space. The closest analogy to a physical domain resides in the equipment separating the edges of the various parts of the domain such as the web servers and firewalls.

The common use of the word network in both definitions is awkwardly ambiguous. With no definition of what a network is existing in any doctrine, the aperture is wide open for interpretation of where the limits of the physical domain intersect with the virtual domain of cyberspace. One person may interpret the network as a system of

systems that includes the people, hardware, computer software, and electronic nodes that connect points in order to share information. Another person may only consider the hardware and the paths to transmit information.

On the surface the subtle differences may not appear significant. However when forced to conduct an analysis of the friendly and enemy centers of gravity in cyberspace, these definitions need to be synchronized in order to determine the correct vulnerabilities to either protect or attack a network in cyberspace.

As previously pointed out, the Marine Corps has not yet published a definition of cyberspace that fits the requirements of the Marine Corps' mission and capabilities. Dr. Lani Kass explained that cyberspace does not just mean computers. It also covers everything from satellite communications to gamma rays to microwave technologies.[9] In another presentation Dr. Kass further described cyberspace as covering "almost everything electrical or electromechanical, from the simplest direct-current applications to the slickest, fastest space-age GPS gadgets off to things that haven't been invented."[10] This opens up the aperture to consider data flowing through fiber optic strands, satellite links, and copper wires. These items are all elements of the physical world.[11] For the purposes of this paper the DoD definition, taking into consideration the limits highlighted by Dr. Kass, will form the basis for all Marine Corps discussions. The term computer network will be defined as any device that transmits an electronic or digital signal containing information to influence actions of people or machines. This allows for not only the inclusion of personal computers, but also radio networks, aircraft data links such as Link 16, and other analogous systems.

III. THREAT ANALYSIS

The Threat to National Security

Two decades ago a person could find American streets speckled with telephone booths and mail boxes. To deposit or withdraw money a person had to go to a bank and obtain assistance from a bank employee. To send a note or letter a person had to sit down with a pen and paper to write a letter and drop it in a mail box so it could be delivered days later to its recipient. Look anywhere in America today and the phone booths are disappearing as people use their personal cellular phones. Bank tellers are not necessary as bank customers do their banking on the Internet or use Automated Teller Machines. E-mail is replacing mail delivered by the US Postal Service. These points demonstrate the difficulty in imagining "a world without instant communications and the freedom to access goods, services, and information at will."[12] Each one of these elements becomes a vulnerability to a potential cyber adversary. A controlled demonstration of the destructive capability of a cyber attack was conducted by the Department of Homeland Security. In this demonstration researchers launched an experimental cyber attack on a power generator causing it to self-destruct. The results of this experiment alarmed federal government and electrical industry officials about what could happen if such an attack were conducted on a larger scale.[13]

The Actors

"America is under widespread attack in cyberspace," according to Gen James C. Cartwright, commander USSTRATCOM.[14] United States Representative Michael McCaul was quoted in a Houston Chronicle interview as saying, "My view is that since September 11 we've been very focused on the physical threats, as we should be, but very

little attention has been paid to the virtual threats—the cyber-attacks to our network systems ranging from mischief to criminal acts or espionage." Representative McCaul went on to say, "With the United States and 24 other countries developing programs to wage war using computers, attacks by foreign governments or terrorists on sensitive U.S. government, critical infrastructure and financial network systems cannot be discounted."[15]

"Our freedom to use cyberspace is threatened by actions of criminals, terrorists and nations alike."[16] Threats to cyberspace come from state and non-state actors. The Internet allows small groups of non-state foes to finance, plan, supply, and execute terrorist operations globally with little regard to borders, laws, and government.[17] China is the number one nation leading global efforts in cyber warfare.[18] As recent as the fall of 2007 cyber attacks traced to Internet addresses in China were reported by the Department of Homeland Security (DHS). The sophisticated fall 2007 attack involved approximately 1,100 attempts to steal data from the Oak Ridge National Laboratory in Tennessee. The attack was classified as a phishing attack[19] where employees were sent two e-mails with legitimate subjects and content regarding a scientific conference and the other a Federal Trade Commission complaint. When the recipient read the e-mail and opened the attached documents an embedded program copied and forwarded information from the computer network to remote locations.[20]

A token non-state actor operating in cyberspace is Al Qaeda.[21] The Internet became the medium of choice for Al Qaeda to coordinate its activities, including the 9/11 attacks.[22] This exemplifies the point that the Internet is a Computer Mediated Communications platform used for recruiting, training, funding, targeting, information

operations, and intelligence collection.[23] Their coordinating measures went beyond websites and e-mail to the use of Internet telephone services to communicate with terror cells overseas. The Internet provided them a place and a means to expand their influence, social network, and operational reach.[24] These same capabilities will be discussed later and illustrate that the Marine Corps has the same capabilities to support their operations.

Threat of Disruption

Paramount to defending cyberspace is preventing the disruption of the flow of communications, economic transactions, and public necessities that foster civilized order such as public utilities. This threat may be to the United States, or any other nation that the Marine Corps happens to be operating in. Much of this disruption would be felt as an economic anomaly; however, the economic stability of a nation is proportional to amount of national civil obedience.

For the United States Marine Corps the disruption of military communications in times of conflict presents the potential loss of life or aborted military missions.[25] The probability of this type of threat cannot be taken lightly as the means to engineer and deliver the threat exists and is becoming easier to exploit.

Threat of Exploitation

Exploitation of information from cyberspace may not strike individuals as a serious matter considering the fact that people use cyberspace daily to distribute information to global audiences. This paper is prepared using a significant amount of information obtained from cyberspace. This information is exploited to make a specific point. Not all examples of exploitation in cyberspace are as benign. For example, in 1999 a series of structured, persistent, and purposeful probes into university, government,

and private sector computer systems in the United States, allegedly originating in Russia, resulted in the theft of considerable amounts of unclassified, but sensitive information. Code name Moonlight Maze, this operation went on for years before it was detected. The attacks were not disruptive, "but dangerous in [the] aggregate."[26] James Adams, Chief Executive Officer of Infrastructure Defense Incorporated testified before the Senate Committee on Governmental Affairs that regarding Moonlight Haze, "The value of this stolen information is in the tens of millions—perhaps hundreds of millions—of dollars; there's really no way to tell. The information was shipped over the Internet to Moscow for sale to the highest bidder. "[27] This example of the uncontrolled release of information for the benefit of a state or non-state actor is significant. Just as significant is the manipulation of data from cyberspace to aid the actor.

Threat of Manipulation

Manipulation of information in cyberspace may not be an obvious threat to military operations. Placing historical events of information manipulation in context makes this an obvious threat. In an cyber attack launched by pro-Palestinian "Pakistani Hackerz Club", members defaced the Web site of the American Israel Public Affairs Committee (AIPAC); they also downloaded 3,500 e-mail addresses to which they sent anti-Israeli messages, and 700 credit card numbers belonging to members who had made donations to the organization and promptly published them on the Internet.[28] While this case may have only served to make a public statement by an independent organization, the social and political impact in regions of the world already socially, politically, and culturally stressed may be enough to trigger second and third order reactions that may prompt a United States military response. As the force in readiness, a Marine Corps

response is an option to the National Leadership to stabilize a region affected by such an attack.

Threat of Destruction

The threat of physical destruction as a result of operations in cyberspace was once considered science fiction and the plot for Hollywood blockbuster films.[29] The reality is that physical destruction as a result of operations in cyberspace has already been documented and will become more sophisticated with time.

Kinetic attacks against power and water distribution networks, sanitation systems, and information networks such as television and radio outlets have been routine targets in the conduct of land-based maneuver warfare. Non-kinetic destruction on these same targets are now inflicted via operations in cyberspace. An example of a low intensity non-kinetic destructive operation in cyberspace was the May 4, 2000 release of the Love Bug computer virus by a 24 year old Philippine man who allegedly developed the password-stealing virus as a school project.[30] The virus not only stole passwords, it deleted files on computers, replicated itself, and used the individuals e-mail address book to distribute itself to every person in the address book. The virus attacked computers worldwide, including computers within the Department of Defense, Department of Commerce, Department of Justice, Department of Health and Human Services, the National Aeronautics and Space Administration, among many others.[31]

Kinetic military operations are no longer required to disrupt critical infrastructure such as power, transportation, and water systems. The Central Intelligence Agency has recently confirmed computer hackers have "in at least one case, caused a power outage affecting multiple cities."[32] This revelation comes only months after the Department of

Homeland Security leaked the report on a controlled experiment where a staged cyber attack demonstrated how easy it is to destroy a power grid. Once access to a computer controlled power grid was gained, a command was sent to one of the generators on the grid. The command directed that the engine increase its revolutions per minute so high that the generator self destructed within minutes.[33] Considering the fragility of civil infrastructure in countries such as Iraq, the threat to non-kinetic cyber attacks producing kinetic results that threatens national security in areas where the Marine Corps is operating requires attention.[34]

The Threat to DoD

While the nation is at war in cyberspace, so is the DoD. General James Cartwright, vice chairman of the Joint Chiefs of Staff, cited statistics on the number of cyber attacks in fiscal year 2007. According to General Cartwright, there were, "80,000 attempted computer network attacks on [DoD] systems."[35] He went on to say that some of these assaults "reduced the U.S., military operational capabilities."[36] In April 1997 the Chinese government formed a cyber hacker army unit who trains specifically for cyber warfare. It has been reported that the Chinese military hackers have mapped out a detailed plan to neutralize U.S. [aircraft] carriers.[37]

This is not the first time that China has been implicated in cyber threats to the DoD. USA Today reported on a DoD program entitled Titan Rain.[38] This program involved a group of researchers in the Guangdong province who coordinated cyberattacks against systems at NASA and Sandia National Laboratories.[39] The Department of Navy was a target of a cyber attack, presumably launched by the Chinese, in fall of 2006. The attack was severe enough that the Naval War College was forced to disconnect from the

Internet for three weeks. Investigators suspect the attackers targeted unclassified information on war games that were being developed at the school.[40]

Relying on a portion of the definition of cyberspace that includes the physical medium that information flows through, the physical security of our satellites that facilitate cyberspace operations cannot be ignored. China poses a threat to satellite security as was illustrated by their successful demonstration of their anti-satellite missile. General Paul Hester, former commander of Pacific Air Forces said that the anti-satellite weapon demonstration is a concern to the US military because of the potential disruption of military communications with commanders in Japan and South Korea.[41] This statement highlights a critical vulnerability to the US military and drives a requirement for DoD action to secure all aspects of cyberspace including the nodal networks in space that enable the cyber battlespace to exist.

Investigations into the cyber attack against Estonia have concluded that Russia may have been responsible for the attack. Moscow denies the charge. The British Broadcasting Corporation (BBC) reported that many of the attacks came from computers hosted by Russian state computer servers.[42] This demonstration of Russian capability highlights an additional threat to the DoD if Russia decides to add this capability to its defense strategy.

IV. INFORMATION MANAGEMENT

The DoD threats from state and non-state actors knows no boundaries. The global nature of information networks yields a ripple effect across the globe when any part is perturbed. An attack on the DoD as a whole is an attack on the Marine Corps as an individual Service. A credible and valid threat exists in cyberspace that threatens the

Marine Corps ability to rapidly process information flowing through the battlespace. The ability to rapidly transfer and process information faster than the enemy is the cornerstone to successful military operations. John Boyd illustrated this point in his studies resulting in the Observe-Orient-Decide-Act (OODA) Loop.[43]

The Marine Corps is developing concepts for future military operations that will rely on rapid and accurate transmission of battlespace information. The amount of information is so great it will require post-processing in order for a human cognitive response. The transfer of this information will occur through cyberspace. The reliance on this information transfer illustrates a need to protect the cyberspace domain to ensure the rapid and accurate transmission of information. Three major concepts that drive the architecture of the future battlespace are highlighted by Distributed Operations (DO), Operational Maneuver From the Sea (OMFTS), and Ship to Objective Maneuver (STOM). Each of these three concepts requires an acknowledgement of cyberspace as a domain to defend and exploit in order to adapt to the tactics of future adversaries or non-combat mission matched to the capabilities of the Marine Corps.

Relationship to Distributed Operations

The concept of DO is controversial to some Marines in the sense that many believe that this is not a new concept and that the Marine Corps has been conducting DO for decades. Despite these views the advanced concept for the future of DO is significant in how it plans to accommodate the threats to its successful implementation.

Distributed Operations relies on the ability of small formations of Marines to move rapidly in space and time while under constant virtual tether with forces adjacent to them, and through their command structures. The ability of a force commander to be

able to command and control the assaulting force is facilitated by information technology that moves data through cyberspace to the adjacent forces and the command chain. The Office of Naval Research highlighted numerous deficiencies in the current DO concept, emphasizing the complexity of the communications networking requirements. Not highlighted in the report were the vulnerabilities associated with operating on a network whose backbone is grounded in cyberspace.[44] Figure one illustrates the complexity associated with the distribution of forces in the battlespace and the associated requirements to have connectivity throughout the battlespace. Enemy activity in cyberspace that targets land, sea, air, space, or cyberspace will cause DO to fail on the same magnitude as not having any capability at all.

Relationship to Operational Maneuver from the Sea

Operational Maneuver From the Sea is a means of gaining advantage over an enemy that aims to exploit a significant enemy weakness in order to deal a decisive blow to an enemy center of gravity.[45] The key requirement for OMFTS is the attainment of an operational level victory. An example of OMFTS was the landing of the Marines at Inchon during the Korean War in order to facilitate the capture of Seoul. The operation was more than a mere tactical victory for the forces that captured the Inchon Port, but an operational victory as well because the focus of the operation was kept on the destruction of the North Korean Army and the liberation of South Korea.[46] The success of this operation was highly dependent on a creative command and control organization and solid intelligence on the status of North Korean forces in South Korea.

Operational Maneuver from the Sea in the 21st Century still relies on robust command and control and accurate and reliable intelligence products. The complexities

of the modern command and control system and intelligence networks are more advanced than the system that Gen MacArthur utilized during the Korean War. None the less the intent of the systems is to reduce the fog of war in order to facilitate a decisive operational victory. The modern battlefield is more complex than ever before. Figure two illustrates a notional deployment of the Marine Expeditionary Force and highlights the complexity of the overlapping networks and the integration of land, sea, air, and space computer networks via exploitation of cyberspace. The complexity and global coverage of the cyber medium required to enable this exceeds the capability of a single person, unit, or military service. There is a role for every Marine operating in this environment to protect the cyber domain in order to ensure operational victory.

Relative to Ship to Objective Maneuver

As a tactical concept within OMFTS, Ship to Objective Maneuver (STOM) takes advantage of mobility and command and control systems to thrust combat power ashore in their fighting formations, to a decisive place, in sufficient strength to ensure mission accomplishment. The requirement to seize a landing zone prior to enemy engagement is not required under the STOM concept.

To accomplish STOM the naval force commander must rely on intelligence and a tactical command and control systems to direct pre-assault operations that will highlight enemy vulnerabilities. Ship to Objective Maneuver exploits the vulnerable gaps of the enemy force.[47] The assumption is made that the intelligence of the enemy disposition and defenses in addition to the current battlespace situation, is accurate when the operation commences. Information is rapidly processed, parsed, and disseminated

between Marine operating forces of the Marine Air Ground Task Force, and higher headquarters often times not located within the same region of the world.

When STOM was first conceived in the 1990's the threat of enemy disruption and corruption of intelligence and command and control systems operating in cyberpace was not a credible threat. Today this is not case. The complexity of the information management and command and control architecture goes beyond line of sight radio frequency communications platforms. The need for parallel combat operations in cyberspace is mandatory to ensure the processing accurate and reliable intelligence of the operating environment in order to facilitate STOM.

V. INFORMATION OPERATIONS

In a 1972 Rand Corporation study, the author concluded, "Whatever the impact of computers on society now, it will be much more profound when everyone or nearly everyone will be using them in the era of mass computer services."[48] This prediction highly underestimated the reality of society only three decades later. The acceptance of computers in society, giving birth to the formation of cyberspace as the medium to facilitate socialization, opens the door to Marine Corps operations that utilize cyberspace to influence the behavior of the society the force operates in. The means to influence societies is through the practice of Information Operations (IO).

Information Operations is defined in the joint community as: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[49] This

definition shows inherent characteristics of both offensive and defensive capabilities. The five components of IO highlighted in the definition have evolved into components that operate in both the physical and virtual (i.e. cyber) operating environments. This affords the opportunity to analyze the credibility of the cyber threats to IO and also assess the impact it has on the ability of the Marine Corps to build and execute an IO mission in support of its expeditionary operations. Although all five components are woven together in cyberspace, operational security and computer network operations require the freedom of maneuver in cyberspace to be successful. This analysis focuses on these two components only. The most logical method of analysis is by looking at examples where cyber threats propagate into the IO arena. At the surface, some of the examples may appear unrealistic; however, none should be discounted considering the rate of change observed in the tactics of cyber warfare activity in the short decade that this threat has been realized.

Operational Security

Sun Tzu said, "If I am able to determine the enemy's dispositions while at the same time conceal my own then I can concentrate and he must divide."[50] Operations Security (OPSEC) is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information. Unlike security programs that seek to protect classified information, OPSEC is a methodology to identify, control, and protect generally unclassified evidence that is associated with sensitive operations and activities.[51]

Threats to OPSEC have been around since the beginning of warfare. Recent examples of external threats to OPSEC are well documented, such as the November 15, 2006 cyber attack on the government computer system at the Naval War College and National Defense University.[52] Internal threats in cyberspace to OPSEC are not as well documented but are easy to imagine. The use of e-mail and the Internet to connect military members around the world is often times as easy in a combat situation as working on a personal computer from their home. The threats associated with OPSEC in cyberspace prompted the DoD to issue a memorandum forbidding the posting of unclassified information and videos to Internet web sites, web logs, on-line personal journals, and other electronic media accessible to the public without first having the content reviewed by Public Affairs.[53]

According to Lt Gen William Caldwell, Commander of the Combined Arms Center, Fort Levenworth, KS, there should be a balance struck between forbidding military members from disseminating information with the threat of potentially harming the lives of fellow warriors, and empowering them through education to publish the friendly message first. He further encourages equipping unit leaders with camcorders to document operations and daily life in order to publish to popular social websites such as YouTube.[54] In a September 2007 Marine Corps Gazette article entitled "Marine Bloggers: Where Are the Guidelines," Capt Stephanie Arndt presented similar conclusions as was presented by Lt Gen Caldwell, but highlighted a feedback relationship that threatens unit OPSEC.[55] Capt Arndt drives home the significance of having a solid IO plan that deliberately takes into account both friendly and enemy threats in cyberspace. The bottom line is that the ability to bring this type of cyber activity into any

Marine unit would exponentially increase the effectiveness of a joint IO campaign, but exposes a vulnerability that every Marine must be aware of before doing battle in this cyber domain.

Computer Network Operation

The pillar that binds all IO activities in cyberspace is Computer Network Operations (CNO). The nature of computer network operations is not bound by geographic, service, or command boundaries. The Marine Corps Network Operations Center is the Marine Corps' component to the joint community's effort to conduct successful warfare in cyberspace. Their mission is to direct global network operations and computer network defense of the Marine Corps Enterprise Network (MCEN).[56] The MCEN enables the Marine Corps to accomplish its global missions in the network-centric battlespace by enabling secure, global information exchange across the full spectrum of operations.

Just as the Marine Corps has a dedicated organization to protect Marine Corps operations in cyberspace, so do state and non-state adversaries. China stood up its own branch within the PLA dedicated to cyber warfare.[57] Although rudimentary in nature, Al Qaeda has experts with the technical knowledge and facilities to produce and disseminate information on the Internet, demonstrating their abilities to wage their own Information Operations campaign.[58] A target of these cyber warriors is the United States DoD and, by association, the Marine Corps. Their sole mission is to disrupt, using their computer networks, the ability of the Marine Corps to accomplish its assigned missions.

Information assurance describes the process of protecting the Marine Corp's critical infrastructure of telecommunications and computer technology.[59] It is the

defensive arm of CNO. Defensive computer network operations are easily understood by most Marines. They will recognize the need to use Public Key Infrastructure (PKI) enabled computer networks, firewalls exist to prevent unauthorized network traffic, and anti-virus software prevents malicious programs from propagating through cyberspace. All of these elements exist to mitigate threats that prevent the Marine Corps from accomplishing its mission. Although easily recognized, it is just as easily taken for granted. Internal threats from transfer of classified information into unclassified networks are just as damaging to computer network operations as an enemy attack.[60]

Our enemy is already conducting offensive operations in cyberspace against the Marine Corps. The DoD has not published any official unclassified reports detailing offensive computer network operations. In an October 15, 2007 Janes Defense Weekly article, USAF Major General William Lord, Commander, United States Air Force Cyber Command, said, "The Air Force plans to work with the Joint Chiefs of Staff over the next 12 to 18 months to streamline the United States government's chain of command so that cyber attacks can be authorized in a matter of minutes." The article continued to quote General Lord, "We'll begin to talk about changing the authority for release of those [cyber] weapons so that ... operationally we can have a much, much quicker turn [around]."[61] This clearly demonstrates that offensive computer network operations are within the realm of possibility for the Marine Corps as the nature of asymmetric warfare continues to evolve.

VI. CONCLUSIONS

The importance of cyberspace is best summed up by Dr. Lani Kass when she said, "If we don't dominate cyberspace, we won't be able to dominate air, space, land or sea

domains."[62] Before domination in cyberspace is possible it has be recognized as a warfighting domain that is just as important as land, sea and air. At this time the Marine Corps has not recognized cyberspace in its doctrine as a warfighting domain for the Marine Corps to dominate. The irony to this observation is every future concept for Marine Corps operations relies on maneuver in cyberspace to facilitate maneuver on land, sea and air. This obvious disconnect needs to be addressed in order to facilitate the full spectrum of military operations that are anticipated to win the Long War. A full discussion of recommendations for improvement can be found at Appendix C.

In order to recognize cyberspace as a warfighting domain, all Marines will need to understand the significance of cyberspace in their assigned mission. They must understand that the ability to rapidly manage information and to use information to influence an adversary's behavior relies on all Marines to contribute to simultaneous offensive and defensive operations in cyberspace while they continue traditional operations across the familiar three dimensional battlespace.

Col John Boyd's OODA Loop is famous for its interpretation by users that the fastest decision cycle wins. Boyd may say this is an oversimplification of his ideas. However, one critical part that is true is that once the cycle begins, it must not slow.[63] Modern asymmetric warfare relies on cyberspace to facilitate the management and manipulation of information used to make decisions. Our future adversaries are not able to manipulate the mind of a Marine, but they can manipulate the information they use to make decisions and slow the Boyd Cycle. The slowing of the cycle may prove disastrous in future conflicts. To avert the forthcoming disaster it is imperative that all Marines recognize that they are not just a riflemen, they are also cyber warriors.

Notes

[1] William Jackson, "The Fourth Dimension: Estonian Official Warns That Cyber Warfare Is a Real Threat." Government Computer News, December 10, 2007, http://www.gcn.com/print/26_30/45520-1.html (accessed December 15, 2007).

[2] *Ibid.*

[3] Arnaud de Borchgrave and others, *Cyber Threats and Information Security: Meeting the 21st Century Challenge* (Washington D.C.: Center for Strategic and International Studies, 2001), 4.

[4] William Gibson, Neuromancer (New York: Ace Books, 1984), 4.

[5] Joint Staff, *DOD Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense), http://www.dtic.mil/doctrine/jel/doddict/index.html (accessed December 29, 2007).

[6] Headquarter United States Air Force, *Air Force Glossary*, AFDD 1-2 (Maxwell AFB, AL: Air Force Doctrine Center), 48, http://www.e-publishing.af.mil/shared/media/epubs/afdd1-2.pdf (accessed December 29, 2007).

[7] Paul Skopowski, Marine Corps Network Operations and Security Center (MCNOSC), interview and briefing, January 11, 2007.

[8] domain. Dictionary.com. *The American Heritage® Dictionary of the English Language, Fourth Edition.* Houghton Mifflin Company, 2004. http://dictionary.reference.com/browse/domain (accessed: February 19, 2008).

[9] Staff Sergeant J. G. Buzanowski. "Cyberspace Expert Briefs AFA Conference Attendees." *Air Force Print News Today*, September 27, 2007. http://www.af.mil/news/story_print.asp?id=123069727 (accessed September 27, 2007).

[10] John Andrew Prime, "Cyber Warfare Oracle Reveals Stark Vision," Republished on-line by HQ USAF AIM Point from The Shreveport Times, http://aimpoints.hq.af.mil/display.cfm?id=21707 (accessed February 25, 2008).

[11] Rebecca Grant, "Victory in Cyberspace" (Arlington, VA: Air Force Association, 2007), 23.

[12] House Armed Services Committee, Subcommittee on Strategic Forces, Statement of General James E. Cartwright, Commaner, United States Strategic Command, 110th Cong, 1st sess., 2007, Committee Print, 4-5, http://armedservices.house.gov/pdfs/FC032107/Cartwright_Testimony032007.pdf (accessed December 18, 2007).

[13] Jeanne Meserve, "Staged Cyber Attack Reveals Vulnerability In Power Grid," http://www.cnn.com/2007/US/09/26/power.at.risk/index.html, (accessed January 21, 2008).

[14] Dave Montgomery, "U.S. Under Widespread Attack In Cyberspace," http://www.innovations.harvard.edu/news/73411.html, (accessed January 21, 2008).

[15] Michelle Mittelstadt, "Texan Fears U.S. Open To Cyber-Attacks: Lawmaker Helps Form Panel To Find Ways To Improve Network Security," http://www.chron.com/CDA/archives/archive.mpl?id=2007_4451688 (accessed February 23, 2008).

[16] House Armed Services Committee, Subcommittee on Strategic Forces, Statement of General James E. Cartwright, Commaner, United States Strategic Command, 110th Cong, 1st sess., 2007, Committee Print, 5.

[17] PowerPoint briefing: Colonel G. I. Wilson, "Terror's Digital Jihad," Webster University, Slide #3, http://www.d-n-i.net/fcs/pdf/wilson_digital_jihad.pdf (accessed January 19, 2008).

[18] Donga.com (South Korea), "China Wants Dominance In Cyber Space," Republished from original source at Donga.com, http://aimpoints.hq.af.mil/display.cfm?id=21379, (accessed September 23, 2007).

[19] Phishing is a form of social engineering. Phishing attacks use email or malicious web sites to solicit personal information. Attackers may send email seemingly from reputable senders that requests information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts. This definition is taken from http://www.us-cert.gov/cas/tips/ST04-014.html (accessed March 7, 2008)

[20] John Markoff, "China Link Suspected In Lab Hacking," New York Times, http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html?partner=rssnyt&emc=rss (accessed December 9, 2007).

[21] William Jackson, "Al Qaeda Set To Meet the Press In Cyberspace," http://www.thestar.com/News/article/287265, (accessed December 24, 2007).

[22] Timothy L. Thomas, "Al Aqeda and the Internet: The Danger of 'Cyberplanning'", Parameters (Spring 2003), http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.htm (accessed January 21, 2008).

[23] PowerPoint briefing: Colonel G. I. Wilson, "Terror's Digital Jihad," slide #9.

[24] Timothy L. Thomas, "Al Aqeda and the Internet: The Danger of 'Cyberplanning'."

[25] Arnaud de Borchgrave and others, *Cyber Threats and Information Security: Meeting the 21st Century Challenge*, (Washington DC: Center for Strategic and International Studies, 2001), 8.

[26] *Ibid.*, 9.

[27] Senate Committee on Governmental Affairs, Testimony of James Adams, Chief Executive Officer, Infrastructure Defense, Inc., 102d Cong., 1st sess., 2000, Committee Print, http://www.senate.gov/~gov_affairs/030200_adams.htm, (accessed February 25, 2008).

[28] *Ibid.*

[29] Examples of such movies are, "Wargames" (1983), "The Net" (1995), "Die Hard IV" (2007).

[30] "Philippine Officials Charge Alleged 'Love Bug' Virus Creator," http://archives.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.html (accessed January 30, 2008).

[31] Diane Frank, "'Love Bug' Uncovers Gaps In Fed Security," http://www.fcw.com/print/6_45/news/70558-1.html (accessed January 30, 2008).

[32] Andy Greenberg, "Hackers Cut Cities' Power," http://www.forbes.com/technology/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html (accessed January 25, 2008).

[33] Jeanne Meserve, "Staged Cyber Attack Reveals Vulnerability In Power Grid."

[34] Steven R. Hurst, "Iraqi Power Grid Near Collapse," http://abcnews.go.com/International/wireStory?id=3447819 (accessed January 30, 2008).

[35] Michael Posner, "America Already Is In a Cyber War, Analyst Says," Republished on-line by HQ USAF AIM Points from National Journal's Technology Daily, http://aimpoints.hq.af.mil/display.cfm?id=22659 (accessed November 28, 2007).

[36] *Ibid*

[37] *Ibid.*

[38] This program was classified until it became public in August 2005. According to the USA Today article the program has since been titled under a new classified name.

[39] Jon Swartz, "Chinese Hackers Seek U.S. Access," http://www.usatoday.com/tech/news/computersecurity/hacking/2007-03-11-chinese-hackers-us-defense_N.htm (accessed January 21, 2008).

[40] *Ibid.*

[41] Bill Gertz, "Chinese Military Boosts Hacking," Republished on-line by HQ USAF AIM Points from the Washington Times, http://aimpoints.hq.af.mil/display.cfm?id=22247 (accessed November 2, 2007)

[42] "Estonia Hit By 'Moscow Cyber War'," http://news.bbc.co.uk/2/hi/europe/6665145.stm, (accessed January 22, 2008).

[43] Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War*, (Boston: Little, Brown and Company, 2002), 334.

[44] Office of Naval Research, "Science and Technology in Support of Naval Distributed Operations: Workshop #2—Final Report 20-21 March 2007," (Arlington, VA: Expeditionary Maneuver Warfare and Combating Terrorism S&T Division, 2007), http://www.onr.navy.mil/sci_tech/30/docs/070521_distributed_operations_workshop_report.pdf (accessed October 15, 2007), 13-14. See also, PowerPoint briefing, "Distributed Operations," slide #14, http://www.onr.navy.mil/nrac/docs/2006_brief_distributed_operations.pdf (accessed October 15, 2007).

[45] *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore*, http://www.dtic.mil/jv2010/usmc/omfts.pdf (accessed February 8, 2008), 5.

[46] *Ibid.*, 9.

[47] United states Marine Corps Warfighting Concepts for the 21st Century, II6-II8.

[48] Harold Sackman, *Computers and Social* Choice, (Santa Monica: The Rand Corporation, 1972), 44.

[49] Joint Electronic Dictionary, s.v. "information operations," http://www.dtic.mil/doctrine/jel/doddict/data/i/02663.html, (accessed January 30, 2008). Definition truncated.

[50] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith, (London: Oxford University Press, 1963), 98.

[51] Joint Chiefs of Staff, *Operations Security.* Joint Publication 3-13.3 (Washington D.C.: Joint Staff, June 29, 2006), http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_3.pdf (accessed February 3, 2008), vii.

[52] Josh Rogin, "Network Attack Disables Naval War College," http://www.fcw.com/online/news/96957-1.html (accessed February 9, 2008).

[53] Secretary of Defense, Information Security/Website Alert, 090426Z AUG 06, http://www.defenselink.mil/webmasters/policy/infosec20060806.html (accessed February 9, 2008).

[54] Lieutenant General William B. Caldwell, "Changing the Organizational Culture (Updated)," posted January 1, 2008, http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/ (accessed February 9, 2008).

[55] Captain Stephanie R. Arndt, "Marine Bloggers: Where Are the Guidelines," *Marine Corps Gazette*, September 2007, 9-10, 12.

[56] The MCEN is the Marine Corps portion of the DoD Global Information Grid.

[57] Donga.com (South Korea), "China Wants Dominance In Cyber Space."

[58] Associated Press, "Al Qaeda Set To Meet the Press In Cyberspace."

[59] Winn Schwartau, *Cybershock: Surviving Hackers, Phreakers, Identity Thieves, Internet Terrorists and Weapons of Mass Disruption*, (New York: Thunder's Mouth Press, 2000), 417.

[60] Lieutenant Colonel Steven Roberts, personal interview, February 15, 2008.

[61] Caitlin Harrington, "USAF Seeks to Speed Up Cyber Attack Process," Republished on-line by HQ USAF AIM Points from Jane's Defense Weekly, http://aimpoints.hq.af.mil/display.cfm?id=21827 (accessed February 25, 2008).

[62] Staff Sergeant J. G. Buzanowski,

[63] Robert Coram, 338.

Appendix A

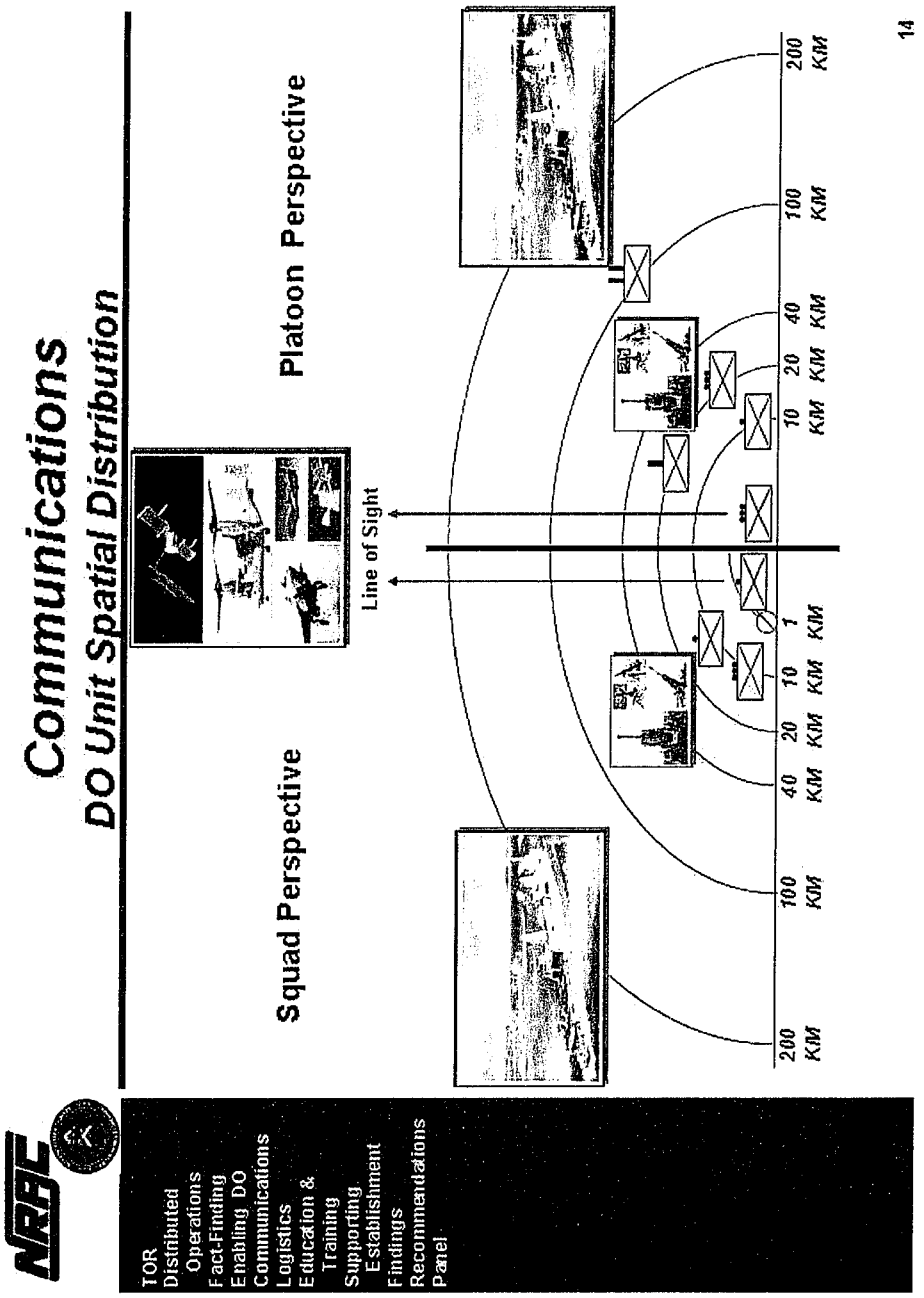

Figure 1. Distributed Operations Unit Spatial Distribution

Slide 14: http://www.onr.navy.mil/nrac/docs/2006_brief_distributed_operations.pdf

Appendix B

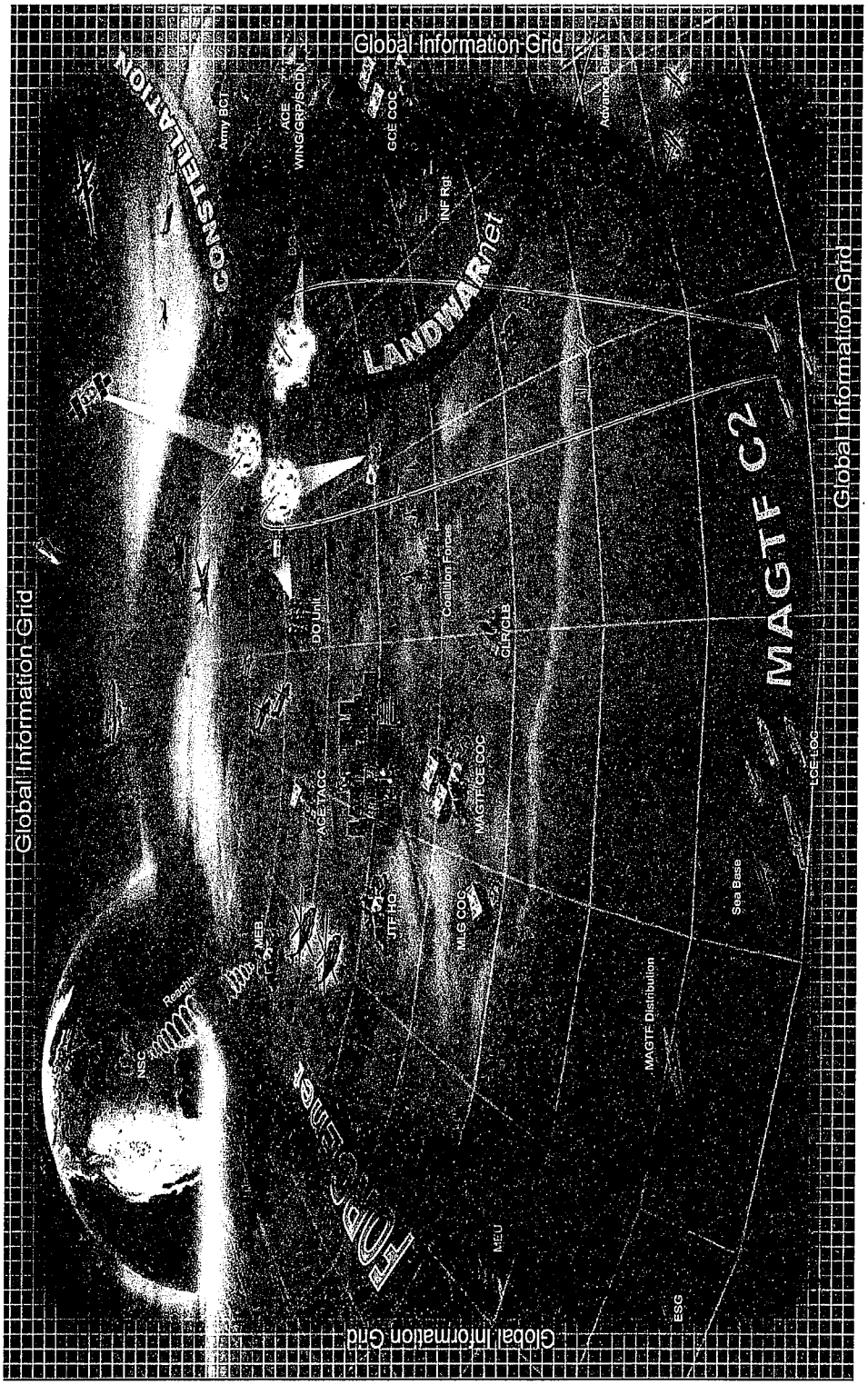

Figure 2. MAGTF C2 Illustration

Appendix C

Recommendations

1. *Codify cyberspace as a warfighting domain in Marine Corps Warfighting Publications.* Once cyberspace is included in doctrine as a warfighting domain it will eventually be engrained in the Marine Corps culture. Once engrained in the culture it will be easy to ensure that planning and execution of future asymmetric conflicts will include defensive, and possible offensive, operations in cyberspace that work to achieve the intent of a joint force commander.

2. *Bolster the Marine Corps education system's curriculum to include the importance of cyberspace and how to exploit this domain.* The current curriculum only scratches the surface of the significance of cyberspace in Marine Corps operations. The ability for the Marine Corps to dominate in cyberspace depends on the involvement of every Marine. To achieve dominance in cyberspace every Marine should have an adequate education on their role in defending the domain.

3. *Every commander must understand their role in defending cyberspace.* The success of operations in cyberspace is laid squarely on the shoulders of every Marine. The commander is responsible for training of every Marine, as well as guiding the appropriate conduct in their duty. If the commander does not ensure their Marines are working in support of effective cyber warfare operations, information management activities, and information operations, the success of the Marine Corps' expeditionary mission is in jeopardy.

4. *Dominance in cyberspace should become a explicit priority of the Marine Corps.* In the February 2007 Marine Corps document entitled, "The Long War: A Marine Corps

Operational Employment Concept to Meet an Uncertain Security Environment," the Commandant of the Marine Corps clearly established his path to successful Marine Corps operations in support of the Long War. The emphasis of the roadmap is to continue to develop capabilities to support a full-spectrum of threats. Highlighted is the probable need for the Marine Corps to mitigate regional instability that impacts our national interest. The document states, "As required, the Marines of the [Security Cooperation] MAGTF will be available for assisting in the development of civil society in ungoverned and under-governed spaces, denying sanctuary to an enemy, conducting operational preparation of the environment, waging ideological warfare, and interdicting terrorists and other irregular enemies."[1] Cyberspace is the medium in which much of civil societies prosper in their daily lives. Information Operations, which has been demonstrated to rely on security in cyberspace, contains the tools necessary to deal with ideological warfare. Offensive cyberspace operations are well suited to support the interdiction of terrorist and other enemies who use cyberspace as a refuge from prosecution. It would be significantly more effective to explicitly declare a priority for the Marine Corps to operate in cyberspace so the proper resources can be applied to the joint effort in support of the Long War

[1] Headquarters United States Marine Corps, "Send in the Marines: A Marine Corps Operational Employment Concept To Meet An Uncertain Security Environment," 20. This document was received by author via e-mail from colleague at Marine Corps Command and Staff College. This document has not yet been posted to the Headquarters United States Marine Corps or the Marine Corps Warfighting Laboratory's websites.

Bibliography

Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore. Washington D.C.: Headquarter United States Marine Corps, n.d., http://www.dtic.mil/jv2010/usmc/omfts.pdf (accessed 2/8/2008).

"Philippine Officials Charge Alleged 'Love Bug' Virus Creator." Cable News Network. http://archives.cnn.com/2000/TECH/computing/06/29/philippines.lovebug.02/index.html (accessed 1/30/2008, 2008).

"China Launches People's Information War :: InfoWar Monitor :: Tracking Cyberpower." http://www.infowar-monitor.net/modules.php?op=modload&name=News&file=article&sid=1470 (accessed 2/9/2008, 2008).

"Domain - Definition from the Merriam-Webster Online Dictionary." http://www.m-w.com/dictionary/domain (accessed 12/31/2007, 2007).

"Estonia Hit by 'Moscow Cyber War'." British Broadcasting Company News. http://news.bbc.co.uk/2/hi/europe/6665145.stm (accessed 1/22/2008, 2008).

"High-Power Microwave (HPM) / E-Bomb." http://www.globalsecurity.org/military/systems/munitions/hpm.htm (accessed 2/17/2008, 2008).

"Information Operations Interview with Dan Kuehl NDU." http://www.iwar.org.uk/infocon/io-kuehl.htm (accessed 1/31/2008, 2008).

"Joint Electronic Dictionary, s.v. "Information Operations "." Joint Staff. http://www.dtic.mil/doctrine/jel/doddict/data/i/02663.html (accessed 1/30/2008, 2008).

"Marching into Cyberspace - Council on Foreign Relations." http://www.cfr.org/publication/15127/marching_into_cyberspace.html?breadcrumb=/publication/publication_list?type=daily_analysis (accessed 12/27/2007, 2007).

"Text Messages Help Nab Iraqi Insurgents - Conflict in Iraq- Msnbc.Com." http://www.msnbc.msn.com/id/6853834/ (accessed 2/10/2008, 2008).

"VoIP for Iraq's Internet Cafés | Quintum Technologies." http://www.quintum.com/providers/iraq-Internet-cafe.html (accessed 1/25/2008, 2008).

Associated Press. "Iraq Wedding-Party Video Backs Survivors' Claims." FoxNews.com. http://www.foxnews.com/story/0,2933,120721,00.html (accessed 2/11/2008, .

Buzanowski, Staff Sergant J. G. "Cyberspace Expert Briefs AFA Conference Attendees." Secretary of the Air Force Public Affairs. http://www.af.mil/news/story_print.asp?id=123069727 (accessed 9/27/2007, 2007).

Caldwell, Lieutenant General William B. *Changing the Organizational Culture (Updated)* (accessed 2/9/2008).

Coll, Steve and Glasser, Susan B. "Terrorists Turn to the Web as Base of Operations." Washington Post. http://www.washingtonpost.com/wp-dyn/content/article/2005/08/05/AR2005080501138.html (accessed 1/25/2008, 2008).

Conway, General James T. *Marine Corps Operating Concepts for a Changing Security Environment*. Washington D.C.: United States Marine Corps, 2007.

Coram, Robert. *Boyd: The Fighter Pilot Who Changed the Art of War*. First ed. Boston, MA: Little, Brown and Company, 2002.

de Borchgrave, Arnaud, Frank J. Cilluffo, Sharon L. Cardash, and Michele M. Ledgerwood. *Cyber Threats and Information Security: Meeting the 21st Century Challenge*. Washington D.C.: Center for Strategic and International Studies, 2001.

Donga.com. "China Wants Dominance in Cyber Space." Republished on-line at USAF AIM Points from original source at Donga.com (South Korea). http://aimpoints.hq.af.mil/display.cfm?id=21379 (accessed 9/23/2007, 2007).

Frank, Diane. "'Love Bug' Uncovers Gaps in Fed Security." Federal Computer Week. http://www.fcw.com/print/6_45/news/70558-1.html (accessed 1/30/2008, 2008).

Friedman, Seargant Major Herbert A. "Psychological Operations during the Israel-Lebanon War 2006." http://www.psywar.org/israellebanon.php (accessed 2/10/2008,

Fulgham, David and Wall, Robert. "Aviation Week : Military Hackers Turn to Commercial Electronic Attack Tools." http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/aw012108p1.xml (accessed 1/25/2008, 2008).

———. "Military Hackers Turn to Commercial Electronic Attack Tools." Republished by HQ USAF AIM Point from Aviation Week and Space Technology. http://aimpoints.hq.af.mil/display.cfm?id=23566 (accessed 1/23/2008, 2008).

Gansler, Jacques S. and Hans Binnendijk, eds. *Information Assurance: Trends in Vulnerabilities, Threats, and Technologies*. Washington D.C.: National Defense University, 2004.

Gertz, Bill. "Chinese Military Boosts Hacking." Republished on-line by HQ USAF AIM Points from the Washington Times. http://aimpoints.hq.af.mil/display.cfm?id=22247 (accessed 11/2/2007, 2007).

Grant, Rebecca. *Victory in Cyberspace*. Arlington, VA: Air Force Association, 2007.

Greenberg, Andy. "Hackers Cut Cities' Power." Forbes. http://www.forbes.com/technology/2008/01/18/cyber-attack-utilities-tech-intel-cx_ag_0118attack.html (accessed 1/25/2008, 2008).

Harrington, Caitlin. "USAF Seeks to Speed Up Cyber Attack Process." Republished on-line by HQ USAF AIM Points from Jane's Defense Weekly. http://aimpoints.hq.af.mil/display.cfm?id=21827 (accessed 2/25/2008, 2008).

Headquarters United States Air Force. *Air Force Glossary*. Maxwell Air Force Base, AL: United States Air Force Doctrine Center, 2007, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1-2.pdf (accessed 12/29/2007).

House Armed Services Committee. *Statement of General James E. Cartwright, Commander, United States Strategic Command, before the Strategic Forces Subcommittee.* 110th Cong., 1st sess. sess., March 8, 2007, 2007.

Hurst, Steven R. "Iraqi Power Grid Nearing Collapse." American Broadcasting Company News. http://abcnews.go.com/International/wireStory?id=3447819 (accessed 1/30/2008, 2008).

Jackson, William. "The Fourth Dimension: Estonian Official Warns that Cyberwarfare is a Real Threat." Government Computer News. http://www.gcn.com/print/26_30/45520-1.html (accessed 12/15/2007, 2007).

———. "Al Qaeda Set to Meet the Press in Cyberspace." http://www.thestar.com/News/article/287265 (accessed 12/24/2007, 2007).

Joint Staff. *Doctrine for Joint Psychological Operations. Joint Publication 3-53.* Washington D.C.: Joint Staff, September 5, 2003, , http://www.dtic.mil/doctrine/jel/new_pubs/jp3_53.pdf (accessed 2/3/2008).

———. "DOD Dictionary of Military and Associated Terms." http://www.dtic.mil/doctrine/jel/doddict/index.html (accessed 12/29/2007, 2007).

———. *Electronic Warfare. Joint Publication 3-13.1.* Washington D.C.: Joint Staff, January 25, 2007, , http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_1.pdf (accessed 2/3/2008).

———. *Operations Security. Joint Publication 3-13.3.* Washington D.C.: Joint Staff, June 29, 2006, , http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13_3.pdf (accessed 2/3/2008).

Joseph, Kristopher. "Defending the Digital Battlefield." http://www.military.com/NewsContent/0,13319,159106,00.html?wh=news (accessed 12/31/2007, 2007).

Kamali, Geoffrey. "*Kenya: Kenyaweb Jumpstarts 20 SMEs.*" http://allafrica.com/stories/200712101359.html (accessed 12/11/2007, 2007).

Kuehl, Dr Daniel. *Information as Power*, http://www.au.af.mil/au/awc/awcgate/navy/nwc_stratcom_conf06/kuehl.pdf (accessed 01/31/2008).

Lachow, Irving and Courtney Richardson. "Terrorist use of the Internet: The Real Story." *Joint Forces Quarterlyint Forces* no. 45 (2nd Quarter, 2007): 100, http://www.ndu.edu/inss/Press/jfq_pages/editions/i45/24.pdf (accessed February 9, 2008).

Markoff, John. "China Link Suspected in Lab Hacking." New York Times. http://www.nytimes.com/2007/12/09/us/nationalspecial3/09hack.html?partner=rssnyt&emc=rss (accessed 12/9/2007, 2007).

Meserve, Jeanne. "Staged Cyber Attack Reveals Vulnerability in Power Grid." http://www.cnn.com/2007/US/09/26/power.at.risk/index.html (accessed 1/21/2008, 2008).

Mittelstadt, Michelle. "Texan Fears U.S. Open to Cyber-Attacks: Lawmaker Helps Form Panel to Find Ways to Improve Network Security." Houston Chronicle. http://www.chron.com/CDA/archives/archive.mpl?id=2007_4451688 (accessed 2/23/2008, 2008).

Montgomery, Dave. "U.S. Under Widespread Attack in Cyberspace." Republished from The Seattle Times, 11/30/2007. http://www.innovations.harvard.edu/news/73411.html (accessed 1/21/2008, 2008).

Nakashima, Ellen. "Bush Order Expands Network Monitoring - Washingtonpost.Com." Washington Post, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/25/AR2008012503261.html?wpisrc=newsletter (accessed 1/26/2008, 2008).

National Oceanic and Atmospheric Administration. "Space Weather." U.S. Department of Commerce. http://www.noaawatch.gov/themes/space.php (accessed 2/17/2008, .

Office of Naval Research. *Science and Technology in Support of Naval Distributed Operations*. Arlington, VA: Expeditionary Maneuver Warfare and Combating Terrorism S&T Division, 2007.

Posner, Michael. "America Already is in a Cyber War, Analyst Says." Republished on-line by HQ USAF AIM Points from National Journal's Technology Daily. http://aimpoints.hq.af.mil/display.cfm?id=22659 (accessed 11/28/2007, 2007).

Prime, John A. "Cyber Warfare Oracle Reveals Stark Vision." Republished on-line by HQ USAF AIM Points from The Shreveport Times. http://aimpoints.hq.af.mil/display.cfm?id=21707 (accessed 2/25/2008, 2008).

Rogin, Josh. "Network Attack Disables Naval War College." http://www.fcw.com/online/news/96957-1.html (accessed 2/9/2008, 2008).

Sackman, Harold. *Computers and Social Choice*. Santa Monica, CA: The Rand Corporation, 1972.

Secretary of Defense. "*Information Security/Website Alert.*" http://www.defenselink.mil/webmasters/policy/infosec20060806.html (accessed 2/9/2008, 2008).

Swartz, Jon. "Chinese Hackers Seek U.S. Access." USA Today. http://www.usatoday.com/tech/news/computersecurity/hacking/2007-03-11-chinese-hackers-us-defense_N.htm (accessed 1/21/2008, 2008).

Thomas, Timothy L. "Al Aqeda and the Internet: The Danger of "Cyberplanning"." *Parameters, US Army War College Quarterly* 33, no. Spring 2003 (: 1/21/2008, http://www.carlisle.army.mil/usawc/Parameters/03spring/thomas.htm (accessed 1/21/2008).

Tzu, Sun. *The Art of War* . Translated by Samuel B. Griffith. London, England: Oxford University Press, 1963.

Commitee on Governmental Affairs. *Testimony of James Adams, Chief Executive Officer, Infrastructure Defense, Inc.* 102d Cong., 1st sess. sess., 03/02/2000, , http://www.senate.gov/~gov_affairs/030200_adams.htm (accessed 2/25/2008).

Wernicke, Carl. "Cyber Warfare is a Real Threat that can Bring Us to our Knees | Opinion | Pnj.Com###." http://www.pensacolanewsjournal.com/apps/pbcs.dll/article?AID=/20080129/OPINION/801290302/1020# (accessed 1/29/2008, 2008).

Wikipedia Contributors. "Wedding Party Massacre." Wikipedia, The Free Encyclopedia. http://en.wikipedia.org/wiki/wedding_party_massacre#_note-ap?oldid=184804411 (accessed 2/11/2008, .

Winn, Patrick. "Hypothetical Attack on U.S. Outlined by China - Air Force News, Opinions, Editorials, News from Iraq, Photos, Reports - Air Force Times." http://www.airforcetimes.com/news/2008/01/airforce_china_strategy_080121/ (accessed 1/21/2008, 2008).